

PATENT APPLICATION TRANSMITTAL LETTER

ATTORNEY'S DOCKET
NO. Rei*1/LUC-163

JC490 U.S. PTO
09/435736
11/08/99

TO THE ASSISTANT COMMISSIONER OF PATENTS AND TRADEMARKS:

Transmitted herewith for filing to the patent application of: Hung et al.

for: **ENCRYPTED AND NON-ENCRYPTED COMMUNICATION OF MESSAGE DATA**

Enclosed are:

20-page Specification, Claims and Abstract
1-page Title page
2-sheets of Informal Drawings
Assignment Transmittal Letter with 1-copy of fee sheet
2-page Executed Assignment
4-page Executed Declaration and Power of Attorney
1 Return Receipt Postcard

FOR	NUMBER FILED	NUMBER EXTRA	RATE	BASIC FEE
TOTAL CLAIMS	28-20 =	8	x \$ 18.00	\$144.00
INDEPENDENT CLAIMS	3-3 =	0	x \$ 78.00	\$.00
ADDITIONAL FEE FOR USE OF MULTIPLE DEPENDENT CLAIM(S) (once per application)			x \$250.00	
			TOTAL FILING FEE	\$904.00
			TOTAL	\$904.00

Original

Continuation-in-part of Serial No. _____

Transfer the drawing(s) from the pending prior application to the application and abandon said prior application as of the filing date accorded this application. An extra (4th) copy of this sheet is enclosed for filing in the prior application file.

Please charge \$904.00 to the Lucent Deposit Account No. 12-2325.

A check in the amount of \$_____ to cover the filing fee is enclosed.

The Commissioner is hereby authorized to charge payment of the following fees associated with this communication credit any overpayment to Deposit Account No. 12-2325.
(Two duplicate copies of this sheet are enclosed.)

Any additional filing fees required using 37 CFR 1.16.

Any patent application processing fees under 37 CFR 1.17.

November 8, 1999
Date

Robert J. Brill
Attorney of Record
Reg. No. 36,760

Robert J. Brill
Signature

SEND CORRESPONDENCE TO:

Robert J. Brill
Wildman, Harrold, Allen & Dixon
225 West Wacker Drive
Chicago, Illinois 60606

CERTIFICATE OF EXPRESS MAIL

"Express Mail" mailing label number EE 434643685US
Date of Deposit. NOVEMBER 8, 1999
I hereby certify that this paper or fee is being deposited with the
United States Postal Service "Express Mail Post Office to
Addressee" on the date indicated above and is addressed to the
Assistant Commissioner for Patents, Washington, D.C. 20231.

Leopolda Lewandowsky
11/8/1999

**APPLICATION FOR UNITED STATES
LETTERS PATENT**

**ENCRYPTED AND NON-ENCRYPTED COMMUNICATION OF
MESSAGE DATA**

By

Arthur Reisman

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the
United States Postal Service by Express Mail No.
EE 434 643685 US in an envelope addressed to the
Commissioner of Patents and Trademarks, Washington, DC 20231.

Date: NOVEMBER 8, 1999

Signed: LEONORA PETROWSKI 

ENCRYPTED AND NON-ENCRYPTED COMMUNICATION OF MESSAGE DATA**TECHNICAL FIELD**

5 This invention relates generally to data communications and more particularly to encrypted communication of data.

BACKGROUND OF THE INVENTION

For encrypted communication of data across the Internet, such as in a commercial context, a user on a client usually logs into a Web page of a Web site having security features.

10 Secure communication of the data entails encryption of all the characters from the Web page. When the user types or inputs data to the Web page, an encryption algorithm is typically employed to process every character. In addition, many or all the characters from the Web page are commonly related by subject or transaction. So, the client often tries to group all the data together for communication of the data. In one example, the data can be transmitted in a same packet and/or as part of a same message. After receiving the encrypted data from the client, the server then performs decryption of the data.

15 However, only a subset of the characters input to a Web page usually comprises sensitive or confidential information. One example of confidential information comprises a social security number or credit card number. The confidential information is encrypted to provide security to the user in the communication or transaction. As one disadvantage, such a configuration consumes processing capacity of the client in encrypting non-confidential data in addition to confidential data. Undesirably, this encryption of the non-confidential data non-productively occupies the processing resource of the client.

20 Such a system has another shortcoming in the form of the required decryption processing by the server of every character sent from the client. To the extent such information is non-

confidential, the additional processing load on the server from the task of decrypting the information consumes processing capacity without providing a benefit. Moreover, the server typically has communication with multiple users. So, the additional processing load for each user multiplies the tasks to be performed by the server. Where the additional processing load 5 from any one or more of the preceding tasks exceeds the immediately available processing power, then overall system performance is disadvantageously slowed. The required decryption of the non-confidential data in addition to the confidential data input by the user can undesirably create a bottleneck. Additional processing to further decrypt non-confidential information from the Web page itself such as description, text, graphics or the like can exacerbate the situation, 10 disadvantageously increasing the bottleneck in the system.

To improve throughput, the Web site usually employs a server having increased processing power. However, the increased processing power of the server requires increased cost for the server. Where the increased processing power results from a requirement to decrypt non-confidential information, then the expense of providing the increased capacity represents a wasteful allocation of resources or funds for the system.

Thus, a need exists for increased efficiency in communication of confidential and non-confidential data.

SUMMARY OF THE INVENTION

Pursuant to the present invention, shortcomings of the existing art are overcome and 20 additional advantages are provided through the provision of communication of a message including a first datum with encryption and a second datum without encryption.

The invention in one embodiment encompasses a method of communicating data between a first computing device and a second computing device. A first datum of a message is

communicated from the first computing device to the second computing device with encryption of the first datum. A second datum of the message is communicated from the first computing device to the second computing device without encryption of the second datum.

Another embodiment of the invention encompasses a data communication system. A first computing device communicates information to a second computing device responsive to a request from the second computing device to the first computing device. The information includes a procedure that causes the second computing device to select a first datum of a message for communication of the first datum from the second computing device to the first computing device with encryption and select a second datum of the message for communication of the second datum from the second computing device to the first computing device without encryption. The first computing device receives the first datum with encryption and the second datum without encryption and decrypts the first datum.

A further embodiment of the invention encompasses an article of manufacture. At least one computer usable medium has computer readable program code means embodied therein for causing communication of a first datum of a message with encryption of the first datum and communication of a second datum of the message without encryption of the second datum. There is provided computer readable program code means for causing a first computing device to communicate information to a second computing device responsive to a request from the second computing device to the first computing device. The information communicated from the first computing device includes a procedure that causes the second computing device to select the first datum of the message for encrypted communication of the first datum from the second computing device to the first computing device and select the second datum of the message for non-encrypted communication of the second datum from the second computing device to the first

computing device. There is also provided computer readable program code means for causing the first computing device to decrypt the first datum of the message communicated with encryption from the second computing device to the first computing device. The second datum of the message is communicated from the second computing device to the first computing device

5 without encryption of the second datum.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a functional block diagram of one example of a communication system including multiple computing devices interconnected by a network.

FIG. 2 is one example of a Web page for communication between a plurality of the multiple computing devices in the system of FIG. 1.

DETAILED DESCRIPTION

In accordance with the principles of the present invention, a first computing device communicates to a second computing device a first datum of a message with encryption of the first datum and a second datum of the message without encryption of the second datum.

Referring to FIG. 1, communication system 100 includes a plurality of computing devices 102. Computing devices 102 are, for instance, interconnected by link 104. In one example, computing devices 102 include one or more instances of server system 106 and client system 108. Link 104 comprises, for example, network 110 interconnecting server system 106 and one 20 or more instances of client system 108. For instance, server system 106 comprises a hypertext transfer protocol (“HTTP”) server. As will be appreciated by those skilled in the art, server system 106 and/or client system 108 can include server as well as client capabilities, features and/or the like. In a further example, each of multiple instances of client system 108 can be connected to network 110 for communication with server system 106 and/or other instances of

client system 108, as will be understood by those skilled in the art. In one example, network 110 comprises a local area network (“LAN”) and/or the Internet. Network 110 includes for example, a plurality of paths or passages 111, which may be static or dynamic, for communication among a number of instances of server system 106 and/or client system 108.

5 Still referring to FIG. 1, STEPS 112, 122, and 132 represent exemplary communication between a client system 108 and a server system 106 such as across a passage 111 of network 110. For example, communication as part of STEPS 112, 122, and/or 132 can include any size and/or amount of information or data. For instance, a datum communicated as part of the information of STEPS 112, 122, and/or 132 can comprise, for example, one or more bits, digits, 10 bytes, words, pages and/or the like.

Further referring to FIG. 1, one example of STEP 112 includes communication of information from client system 108 across network 110 to server system 106. User 114 employs link 116 to interface with client system 108. Client system 108 includes browser 118. For instance, the information of STEP 112 comprises a request from user 114. User 114 employs browser 118 to communicate the request as part of STEP 112. For example, user 114 employs link 116 to access browser 118 for logging into Web site 120, as described herein. Link 121 interconnects Web site 120 and server system 106.

Referring again to FIG. 1, STEP 122 includes server system 106 communicating across network 110 to client system 108. For example, STEP 122 includes server system 106 responding to the request from client system 108 as part of STEP 112. In response to the request from client system 108 in STEP 112, for example, server system 106 prepares or selects information for client system 108 such as Web page 124, procedure or embedded program 126, and first and second keys. For instance, the first and second keys allow security in

communication such as through encryption and decryption of transmitted data, as in STEPS 122 and/or 132. In one example, the first and second keys comprise public key 128 and private key 130. For instance, embedded program 126, public key 128, and private key 130 comprise an encryption algorithm and matched keys based on RSA. Web page 124 comprises, for instance, 5 hypertext markup language (“HTML”). In one example, embedded program 126 can be sent or transmitted with Web page 124. Embedded program 126 is implemented in, for example, a machine independent programming language such as Java, from Sun Microsystems. For instance, embedded program 126 is implemented with a Java applet. In one example, embedded program 126 employs lowest or substantially lowest common denominator Java. Embedded program 126 uses, for example, basic or the most basic Java utilities and a simple or very simple 10 Java application to promote compatibility with multiple and various types of browser 118 on different instances of client system 108. As one advantage, this compatibility promotes avoidance of delays in communication which might otherwise arise in the event of incompatibilities such as among various browsers 118 and/or computing devices 102, as will be appreciated by those skilled in the art. In another example, embedded program 126 is 15 implemented with ActiveX, from Microsoft Corporation.

Further referring to FIG. 1, one example of STEP 122 includes server system 106 communicating information to client system 108 comprising Web page 124. Server system 106 communicates Web page 124 across network 110 in STEP 122 as a response to the request from 20 client system 108 in STEP 112. In one example, Web page 124 communicated to client system 108 includes embedded program 126. Embedded program 126 communicated to client system 108, in one example, employs public key 128.

Referring again to FIG. 1, client system 108 employs or runs embedded program 126 of Web page 124 communicated from server system 106 in STEP 122. Embedded program 126 employs public key 128 on client system 108 to encrypt confidential or sensitive data provided by user 114, as described herein. In one example, embedded program 126 advantageously 5 encrypts confidential data provided by user 114 without encrypting non-confidential data provided by user 114.

Still referring to FIG. 1, STEP 132 includes client system 108 communicating information, for instance, a message, to server system 106. The message communicated from client system 108 to server system 106 comprises information input from user 114 to Web page 124 on client system 108. In one example, the information comprising the message includes data having a relation, such as by subject, matter, transaction, occurrence or the like.

Referring further to FIG. 1, STEPS 112, 122, and 132 in one example employ a same passage 111 of network 110 between client system 108 and server system 106. For instance, this passage 111 can cross and/or comprise the Internet and/or conform to a networking protocol such as transmission control protocol/Internet protocol (“TCP/IP”). In one example, STEPS 112, 122, and 132 are performed across a same TCP/IP socket comprising a passage 111. In a further example, any one of STEPS 112, 122, and/or 132 can comprise a single packet of a message, or a plurality of packets of a message, as will be appreciated by those skilled in the art.

Turning to FIG. 2, Web page 124 in one example comprises a plurality of portions 202. 20 For instance, portions 202 include a number of entry fields 204 and a number of presentation fields 206. For instance, one or more entry fields 204 allow user 114 (FIG. 1) to input characters or text. One or more presentation fields 206 comprise, for instance, a prompt, instruction, entertainment, direction, advertisement, announcement and/or the like. For example, one or

more presentation fields 206 can comprise text and/or graphics to request and/or direct input of information by user 114 into one or more entry fields 204.

For illustrative purposes, a detailed description of exemplary operation of communication system 100 is presented with reference to FIGS. 1-2.

5 Referring to FIGS. 1-2, user 114 decides to apply for a credit card as a request in STEP 112. User 114 employs link 116 to use browser 118 on client system 108. Browser 118 allows user 114 to interface with client system 108 and employ server system 106 across network 110 to access Web site 120. In one example, Web site 120 provides an icon (not shown) that user 114 selects with a pointer (not shown) controlled by a mouse (not shown). User 114 activates the icon by clicking a button (not shown) on the mouse. The activation of the icon by user 114 comprises a request from client system 108 to server system 106 as part of STEP 112, as will be appreciated by those skilled in the art.

10 Referring still to FIGS. 1-2, server system 106 receives the request from client system 108 as part of STEP 112. Since the request from client system 108 comprises a request for a credit card, server system 106 determines or knows that confidential information as well as non-confidential information will be communicated in STEP 132 across network 110 between client system 108 and server system 106. For instance, the confidential information comprises information about user 114 that user 114 wishes to share only with a company responsible for Web site 120. The company with which user 114 wishes to share the confidential information 15 comprises a company with which user 114 wishes to pursue, for example, a commercial transaction or authorization such as an application for, or purchase by use of, a credit card. In addition, during STEP 132 user 114 wishes to keep the confidential information secret or private 20 from any party other than the company responsible for Web site 120. To provide security for

communication of the confidential information from user 114 across network 110, server system 106 in STEP 122 communicates embedded program 126 with public key 128 and Web page 124 to client system 108. User 114 employs link 116 to access Web page 124 on client system 108.

Again referring to FIGS. 1-2, in one example server system 106 employs a same key as 5 public key 128 for each credit card request received from a number of client systems 108. For instance, the same key as public key 128 can be employed over a period such as one hour, one day, or one week. At the conclusion of the selected period, a different key as public key 128 can be employed until a conclusion of a subsequent period. In addition, server system 106 can use a same key as private key 130 coordinated with public key 128 for decryption of each 10 communication from client system 108, for instance, occurring or commenced in the particular time period. As a further example, a same key can be employed as public key 128 for a certain number of requests received as part of a number of occurrences of STEP 112. A same basis would be employed to update a particular key for private key 130. In another example, server system 106 dynamically generates or provides a distinct set of keys as a matched key 128 and 15 private key 130 for each user 114 transmitting or sending a credit card request, or for each such request sent, to server system 106 as part of STEP 112. In such a case, server system 106 could include a cookie (not shown) in the communication as part of STEP 122. Further, client system 108 could employ the cookie in the communication of STEP 132 to allow server system 106 to 20 keep track of user 114. Also, the cookie returned in STEP 132 would allow server system 106 to match the particular private key 130 with the public key 128 for decryption of the confidential data from the corresponding user 114, as will be understood by those skilled in the art.

Further referring to FIGS. 1-2, a presentation field 206 may include text asking or directing user 114 to input an address of user 114 into a certain entry field 204. In one example,

the data from the particular presentation field 206 and corresponding entry field 204 concerning the address of user 114 comprise non-confidential information.

Referring again to FIGS 1-2, in one example embedded program 126 recognizes this particular presentation field 206 and corresponding entry field 204 concerning the address 5 information of user 114 as comprising non-confidential data. So, embedded program 126 determines or selects that this address information of user 114 be treated as non-confidential data for communication as part of STEP 132. For STEP 132, embedded program 126 abstains from applying an encryption algorithm to the non-confidential data. Advantageously, a processor (not shown) on client system 108 need not perform encryption processing on the non-confidential data. The non-confidential data is communicated in STEP 132 without encryption. This non-encryption of the non-confidential data for communication in STEP 132 also provides a savings in processing to be performed by server system 106. Advantageously, a processor (not shown) on server system 106 need not perform decryption processing on the non-confidential data communicated in STEP 132. Desirably, the processors on server system 106 and client system 108 are therefore relieved or freed, for example, to perform other processing and/or be sized to require less processing power. As another example, the processor of server system 106 is advantageously allowed to handle other or additional STEPS 132 from different client systems 108 each demanding reduced processing power from server system 106 since the non-confidential data arrive at server system 106 without encryption while the confidential data 20 arrives with encryption, as described herein.

Referring further to FIGS. 1-2, Web page 124 comprises a presentation field 206 including text that, for example, requests or directs user 114 to input a social security number of user 114 into a particular entry field 204. In one example, the social security number of user 114

input into the designated entry field 204 comprises confidential data. Optionally, the text in the presentation field 206 requesting or directing user 114 to input the social security number into entry field 204 can be considered to comprise confidential data. In one example, embedded program 126 represents or implements a design choice that selects or determines which one or 5 more subsets of entry fields 204 and/or presentation fields 206 include confidential data. Advantageously, embedded program 126 employs an encryption algorithm to encrypt the confidential data from these one or more subsets of entry fields 204 and/or presentation fields 206 for communication as part of STEP 132. In addition, embedded program 126 advantageously abstains or refrains from encrypting the non-confidential data for communication as part of STEP 123.

10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95

20

Still referring to FIGS. 1-2, user 114 through link 116 inputs data into each of entry fields 204. As described herein, a subset of portions 202 comprise confidential data. After user 114 completes inputting data into entry fields 204, user 114 indicates a readiness to send the data such as by highlighting and activating or clicking an icon designated as a send button (not shown). In one example of STEP 132, the activation of the send button starts an encryption algorithm in embedded program 126. The activation of the encryption algorithm in embedded program 126 causes embedded program 126 to encrypt confidential data from the subset of portions 202 determined to be confidential and refrain from encrypting the remainder of portions 202 besides or except this subset of portions 202 selected or designated as comprising the confidential data.

20

Although preferred embodiments have been depicted and described in detail herein, it will be apparent to those skilled in the relevant art that various modifications, additions, substitutions and the like can be made without departing from the spirit of the invention and

these are therefore considered to be within the scope of the invention as defined in the following claims.

CLAIMS

What is claimed is:

1. A method of communicating data between a first computing device and a second computing device, the method comprising the steps of:

communicating a first datum of a message from the first computing device to the second computing device with encryption of the first datum; and

communicating a second datum of the message from the first computing device to the second computing device without encryption of the second datum.

10 2. The method of claim 1 wherein the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the message without encryption of the second datum comprise the step of communicating the first datum with encryption and the second datum without encryption in a same packet that comprises the message.

15 3. The method of claim 1 wherein the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the message without encryption of the second datum comprise the steps of:

communicating the first datum with encryption in a first packet of the message;

and

20 communicating the second datum without encryption in a second packet of the message different from the first packet of the message.

4. The method of claim 1 wherein the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of

the message without encryption of the second datum comprise the step of employing a same path between the first computing device and the second computing device to communicate the first datum with encryption and the second datum without encryption.

5. The method of claim 4 wherein the step of employing the same path to communicate the first datum with encryption and the second datum without encryption comprises the step of employing a TCP/IP passage between the first computing device and the second computing device to communicate the first datum with encryption and the second datum without encryption.

6. The method of claim 1 wherein the step of communicating the first datum of the message with encryption of the first datum comprises the step of employing a key to encrypt the first datum of the message for communication of the first datum from the first computing device to the second computing device with encryption of the first datum.

7. The method of claim 1 further comprising the step of communicating a key from the second computing device to the first computing device, and wherein the step of communicating the first datum of the message from the first computing device to the second computing device with encryption of the first datum comprises the step of employing the key to encrypt the first datum of the message for communication of the first datum from the first computing device to the second computing device.

8. The method of claim 7 wherein the key comprises a first key, and further comprising the step of employing a second key to decrypt the first datum of the message after communication of the first datum from the first computing device to the second computing device with encryption of the first datum.

9. The method of claim 8 further comprising the step of selecting the first key and the second key to comprise matched keys for communication of the first datum of the message from the first computing device to the second computing device with security of the first datum.

10. The method of claim 1 further comprising the step of communicating a procedure 5 from the second computing device to the first computing device, and wherein the step of communicating the first datum of the message from the first computing device to the second computing device with encryption of the first datum comprises the step of employing the procedure to encrypt the first datum of the message for communication of the first datum from the first computing device to the second computing device.

11. The method of claim 10 wherein the step of communicating the procedure from the second computing device to the first computing device comprises the step of selecting the procedure to comprise a procedure based on a machine independent Web protocol.

12. The method of claim 10 wherein the step of communicating the procedure from the second computing device to the first computing device comprises the step of selecting the procedure to comprise a procedure based on substantially lowest common denominator Java.

13. The method of claim 10 wherein the step of communicating the first datum of the message from the first computing device to the second computing device with encryption of the first datum comprises the step of employing the procedure to select the first datum of the message for communication of the first datum from the first computing device to the second computing device with encryption of the first datum.

20 14. The method of claim 13 wherein the step of communicating the second datum of the message from the first computing device to the second computing device without encryption of the second datum comprises the step of employing the procedure to select the second datum of

the message for communication of the second datum from the first computing device to the second computing device without encryption of the second datum.

15. A data communication system comprising:

5 a first computing device that communicates information to a second computing device responsive to a request from the second computing device to the first computing device, the information including a procedure that causes the second computing device to select a first datum of a message for communication of the first datum from the second computing device to the first computing device with encryption and select a second datum of the message for communication of the second datum from the second computing device to the first computing device without encryption; and

10 the first computing device receiving the first datum with encryption and the second datum without encryption and decrypting the first datum.

15. The system of claim 15 wherein the first computing device receives the first datum with encryption and the second datum without encryption in a same packet that comprises the message.

20 17. The system of claim 15 wherein the first computing device receives the first datum with encryption in a first packet of the message, and wherein the first computing device receives the second datum without encryption in a second packet of the message different from the first packet of the message.

18. The system of claim 15 wherein the first computing device employs a same path to receive from the second computing device, the first datum of the message with encryption and the second datum of the message without encryption.

19. The system of claim 18 wherein the same path comprises a TCP/IP passage between the first computing device and the second computing device.

20. The system of claim 15 wherein the information communicated from the first computing device to the second computing device includes a key employed by the second computing device to encrypt the first datum of the message for communication of the first datum from the second computing device to the first computing device.

21. The system of claim 20 wherein the key comprises a first key, and wherein the first computing device employs a second key to decrypt the first datum of the message communicated from the second computing device to the first computing device with encryption of the first datum.

22. The system of claim 21 wherein the first computing device selects the first key and the second key to comprise matched keys for communication of the first datum of the message from the second computing device to the first computing device with security of the first datum.

23. The system of claim 15 in combination with the second computing device, wherein the second computing device employs the procedure to encrypt the first datum for communication of the first datum of the message from the second computing device to the first computing device.

24. The system of claim 15 wherein the procedure is based on a machine independent Web protocol.

25. The system of claim 15 wherein the procedure is based on substantially lowest common denominator Java.

26. The system of claim 15 wherein the procedure causes the second computing device to select the first datum for communication of the first datum of the message from the second computing device to the first computing device with encryption of the first datum.

27. The system of claim 26 wherein the procedure causes the second computing device to select the second datum for communication of the second datum of the message from the second computing device to the first computing device without encryption of the second datum.

28. An article of manufacture, comprising:

at least one computer usable medium having computer readable program code means embodied therein for causing communication of a first datum of a message with encryption of the first datum and communication of a second datum of the message without encryption of the second datum, the computer readable program code means in the article of manufacture comprising:

computer readable program code means for causing a first computing device to communicate information to a second computing device responsive to a request from the second computing device to the first computing device, the information including a procedure that causes the second computing device to select the first datum of the message for encrypted communication of the first datum from the second computing device to the first computing device and select the second datum of the message for non-encrypted communication of the second datum from the second computing device to the first computing device; and

computer readable program code means for causing the first computing device to decrypt the first datum of the message communicated with encryption from the second

10
15
20

computing device to the first computing device, the second datum of the message communicated without encryption from the second computing device to the first computing device.

6 6 8 0 0 T T = 0 0 0 0 0 0 0 0 0 0 0 0

ENCRYPTED AND NON-ENCRYPTED COMMUNICATION OF MESSAGE DATA

ABSTRACT OF THE DISCLOSURE

A first datum of a message is communicated from a first computing device to a second computing device with encryption of the first datum. A second datum of the message is communicated from the first computing device to the second computing device without encryption of the second datum. In one example, the second computing device communicates information to the first computing device responsive to a request from the first computing device to the second computing device. The information includes a procedure that causes the first computing device to select the first datum for encrypted communication to the second computing device and select the second datum for non-encrypted communication to the second computing device.

Erg. 1

104

HTTP Server

Unique Client

Session generates 126
form , Java App,
public and private keys
127
128

Decryption
done with
unique private
key

106 →

The Internet

5

CUSTOMER LOGS WED 3/13 110

~ 114 ~

Rei*VLUC-163

1 / 2

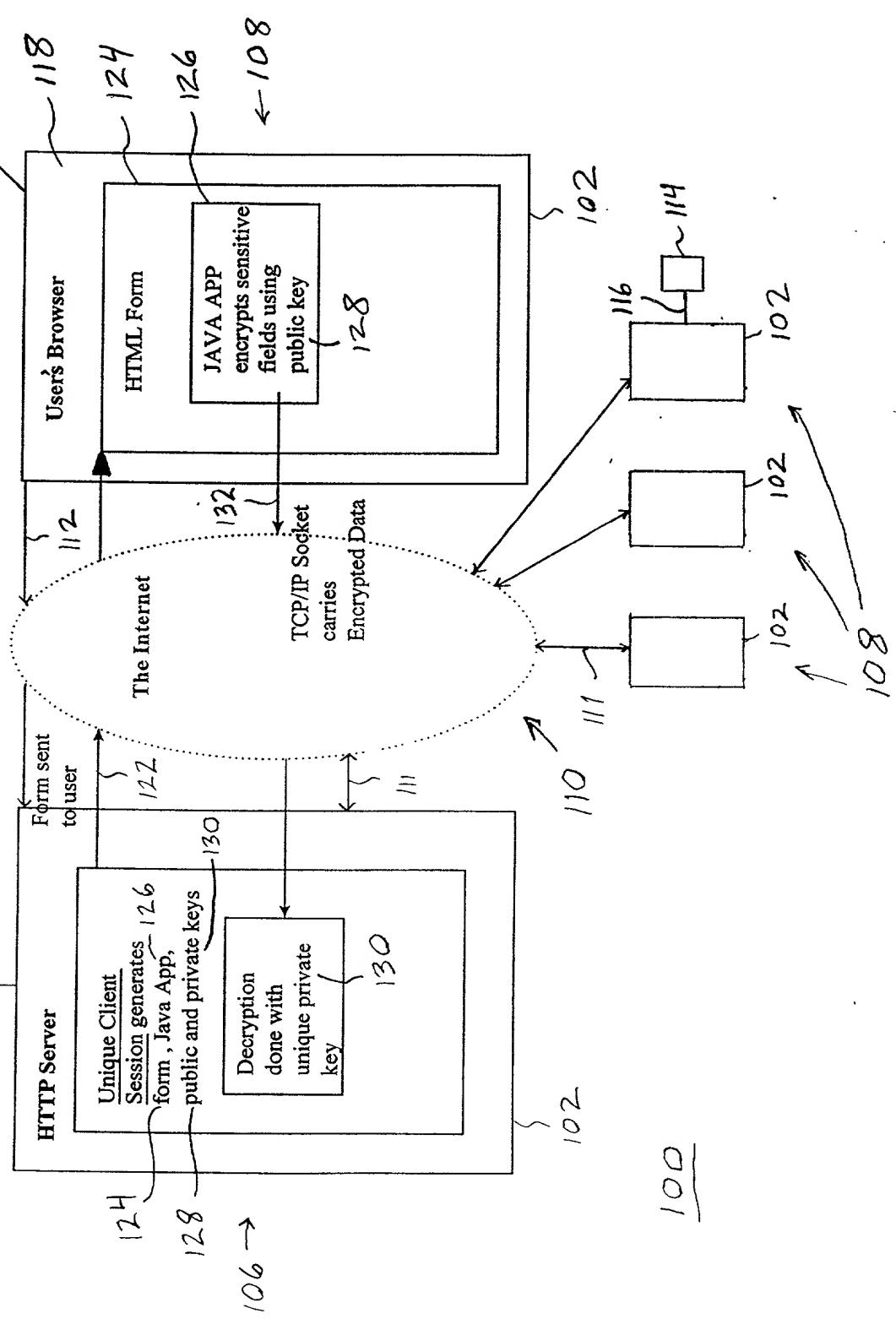
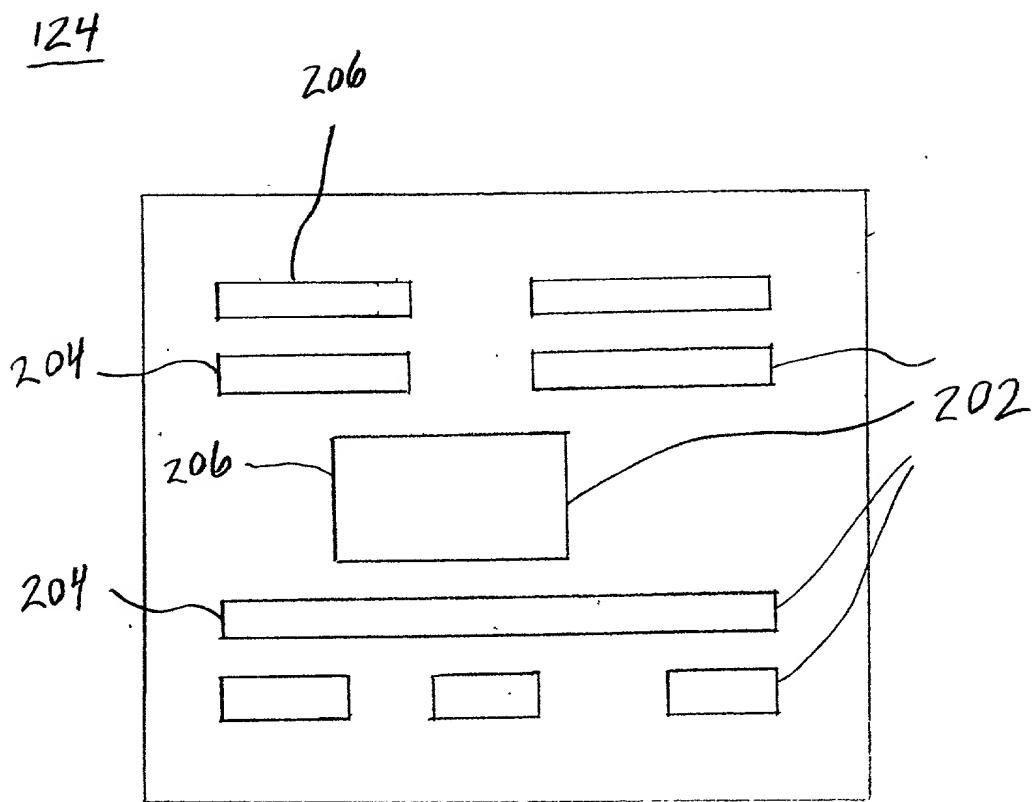


FIG. 2

2/2
Rei*1/LUC-163



IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

Declaration and Power of Attorney

As the below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled **ENCRYPTED AND NON-ENCRYPTED COMMUNICATION OF MESSAGE DATA** the specification of which is attached herewith.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by an amendment, if any, specifically referred to in this oath or declaration.

I acknowledge the duty to disclose all information known to me which is material to patentability as defined in Title 37, Code of Federal Regulations, 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

None

I hereby claim the benefit under Title 35, United States Code, 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

None

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I hereby appoint the following attorney(s) with full power of substitution and revocation, to prosecute said application, to make alterations and amendments therein, to receive the patent, and to transact all business in the Patent and Trademark Office connected therewith:

Lester H. Birnbaum	(Reg. No. 25830)
Richard J. Botos	(Reg. No. 32016)
Jeffery J. Brosemer	(Reg. No. 36096)
Kenneth M. Brown	(Reg. No. 37590)
Craig J. Cox	(Reg. No. 39643)
Donald P. Dinella	(Reg. No. 39961)
Guy Eriksen	(Reg. No. 41736)
Martin I. Finston	(Reg. No. 31613)
James H. Fox	(Reg. No. 29379)
William S. Francos	(Reg. No. 38456)
Barry H. Freedman	(Reg. No. 26166)
Julio A. Garceran	(Reg. No. 37138)
Mony R. Ghose	(Reg. No. 38159)
Jimmy Goo	(Reg. No. 36528)
Anthony Grillo	(Reg. No. 36535)
Stephen M. Gurey	(Reg. No. 27336)
John M. Harman	(Reg. No. 38173)
Michael B. Johannesen	(Reg. No. 35557)
Mark A. Kurisko	(Reg. No. 38944)
Irena Lager	(Reg. No. 39260)
Christopher N. Malvone	(Reg. No. 34866)
Scott W. McLellan	(Reg. No. 30776)
Martin G. Meder	(Reg. No. 34674)
John C. Moran	(Reg. No. 30782)
Michael A. Morra	(Reg. No. 28975)
Gregory J. Murgia	(Reg. No. 41209)
Claude R. Narcisse	(Reg. No. 38979)
Joseph J. Opalach	(Reg. No. 36229)
Neil R. Ormos	(Reg. No. 35309)
Eugen E. Pacher	(Reg. No. 29964)
Jack R. Penrod	(Reg. No. 31864)
Daniel J. Piotrowski	(Reg. No. 42079)
Gregory C. Ranieri	(Reg. No. 29695)
Scott J. Rittman	(Reg. No. 39010)
Eugene J. Rosenthal	(Reg. No. 36658)
Bruce S. Schneider	(Reg. No. 27949)
Ronald D. Slusky	(Reg. No. 26585)
David L. Smith	(Reg. No. 30592)
Patricia A. Verlangieri	(Reg. No. 42201)
John P. Veschi	(Reg. No. 39058)
David Volejnicek	(Reg. No. 29355)
Charles L. Warren	(Reg. No. 27407)
Jeffrey M. Weinick	(Reg. No. 36304)
Eli Weiss	(Reg. No. 17765)

I hereby appoint the attorney(s) on ATTACHMENT A as associate attorney(s) in the aforementioned application, with full power solely to prosecute said application, to make alterations and amendments therein, to receive the patent, and to transact all business in the Patent and Trademark Office connected with the prosecution of said application. No other powers are granted to such associate attorney(s) and such associate attorney(s) are specifically denied any power of substitution or revocation.

Full name of sole inventor: Arthur Reisman

Inventor's
signature

Art Reisman

Date 11/5/99

Residence: New Albany, Franklin County, Ohio

Citizenship: USA

Post Office Address: 8063 Clouse Road
New Albany, Ohio 43054

662017-98255610

ATTACHMENT A

Attorney Name(s):	<u>Carmen B. Patti</u>	Reg. No.:	<u>26,784</u>
	<u>Thomas J. Ring</u>		<u>29,971</u>
	<u>Gary R. Gillen</u>		<u>35,157</u>
	<u>Scot R. Hewitt</u>		<u>35,191</u>
	<u>Robert J. Brill</u>		<u>36,760</u>
	<u>Gregory B. Gulliver</u>		<u>44,138</u>

Telephone calls should be made to Wildman, Harrold, Allen & Dixon at:

Phone No.: 312/201.2257

Fax No.: 312/201.2555

All written communications are to be addressed to:

Wildman, Harrold, Allen & Dixon
225 West Wacker Drive
Chicago, Illinois 60606

SUSPECT IDENTIFIED